Configuración de SSL AnyConnect Management VPN en FTD

Contenido

Introducción

Este documento describe cómo configurar un túnel de Cisco AnyConnect Management en Cisco Firepower Threat Defense (FTD) que se administra mediante Cisco Firepower Management Center (FMC). En el ejemplo siguiente, Secure Sockets Layer (SSL) se utiliza para crear una red privada virtual (VPN) entre FTD y un cliente Windows 10.

Colaborado por Daniel Perez Vertti Vazquez, Ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Editor de perfiles de Cisco AnyConnect
- Configuración de SSL AnyConnect a través de FMC.
- Autenticación de certificado de cliente

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco FTD versión 6.7.0 (versión 65)
- Cisco FMC versión 6.7.0 (versión 65)
- Cisco AnyConnect 4.9.01095 instalado en el equipo Windows 10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Desde la versión 6.7, Cisco FTD admite la configuración de los túneles de AnyConnect Management. Esto corrige la solicitud de mejora previamente abierta CSCvs78215.

La función AnyConnect Management permite crear un túnel VPN inmediatamente después de que el terminal finalice su inicio. No es necesario que los usuarios inicien manualmente la aplicación AnyConnect, tan pronto como se enciende el sistema, el servicio de agente AnyConnect VPN detecta la función Management VPN e inicia una sesión AnyConnect mediante la entrada Host definida en la lista de servidores del perfil VPN de administración de AnyConnect.

Limitaciones

- Solo se admite la autenticación de certificado de cliente.
- Sólo los clientes de Windows admiten el almacén de certificados de equipo.
- No se admite en Cisco Firepower Device Manager (FDM) CSCvx90058.
- No soportado en clientes Linux.

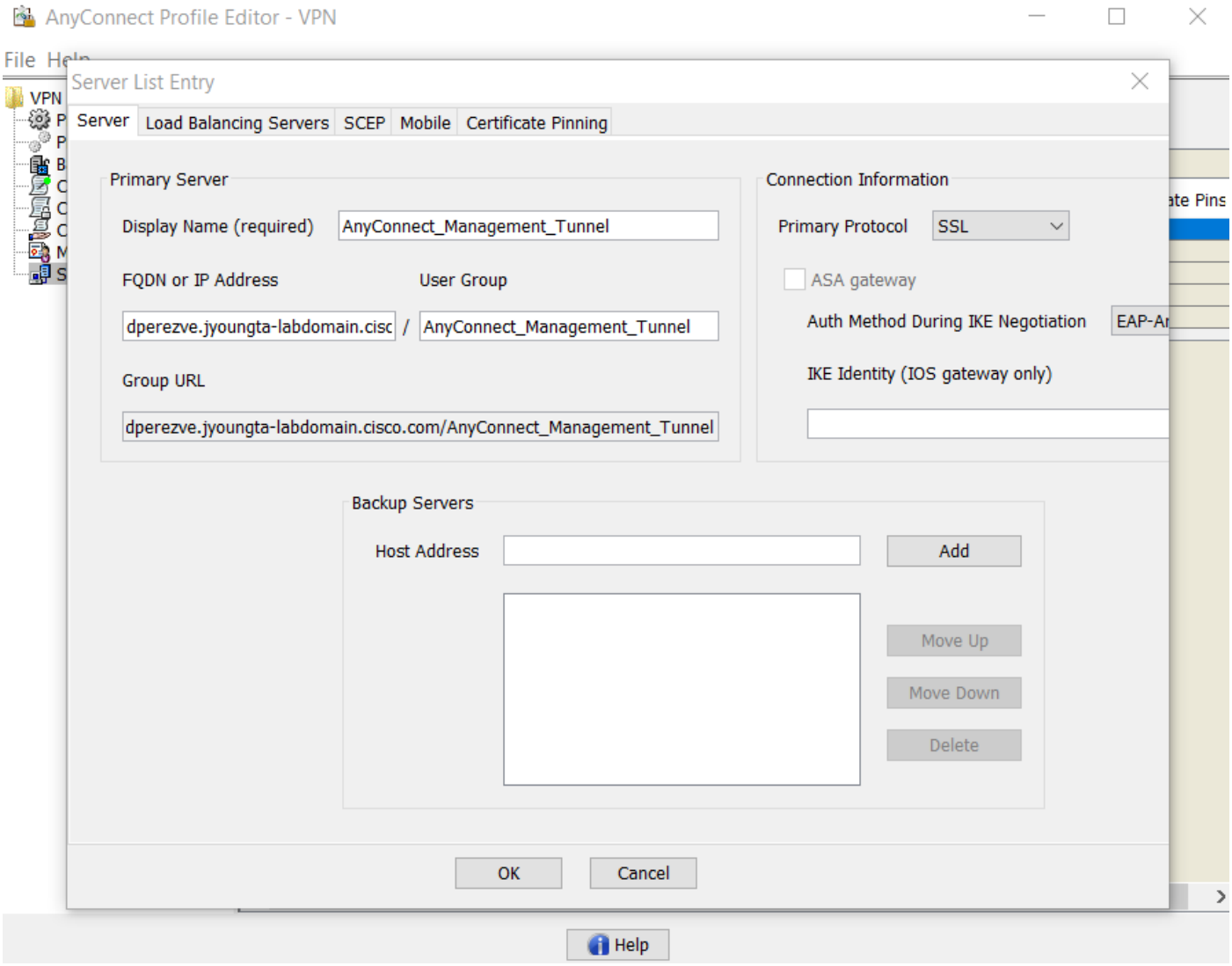
Configurar

Configuraciones

Paso 1. Crear el perfil VPN de administración de AnyConnect

Abra el Editor de perfiles de AnyConnect para crear el perfil VPN de administración de AnyConnect. El perfil de administración contiene todos los ajustes utilizados para establecer el túnel VPN después de que se inicie el terminal.

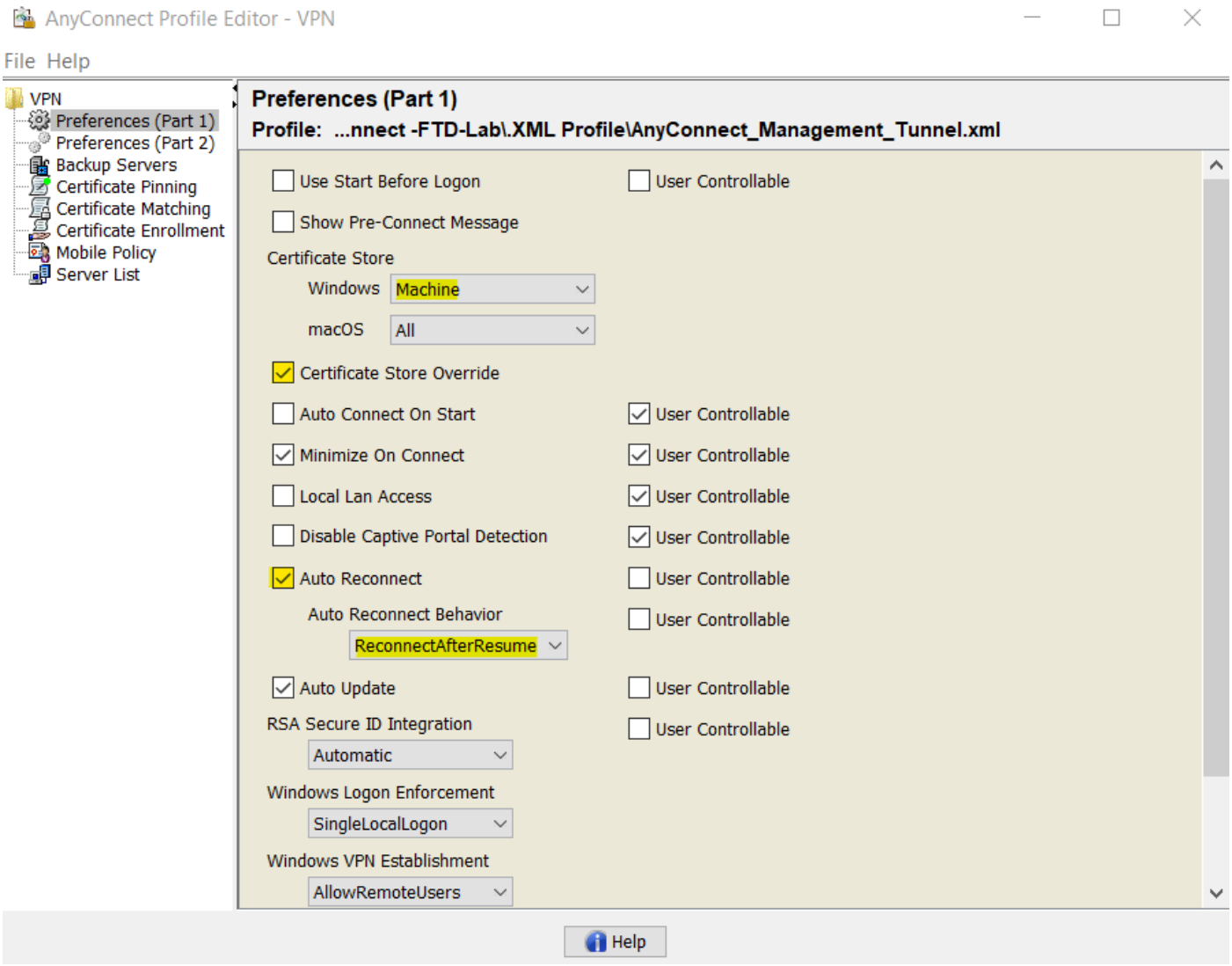
En este ejemplo, se define una entrada de lista de servidores que apunta a Nombre de dominio completo (FQDN) dperezve.jyoungta-labdomain.cisco.com y se selecciona SSL como el protocolo principal. Para agregar una lista de servidores, navegue hasta **Lista de servidores** y seleccione el botón **Agregar** , rellene los campos obligatorios y guarde los cambios.



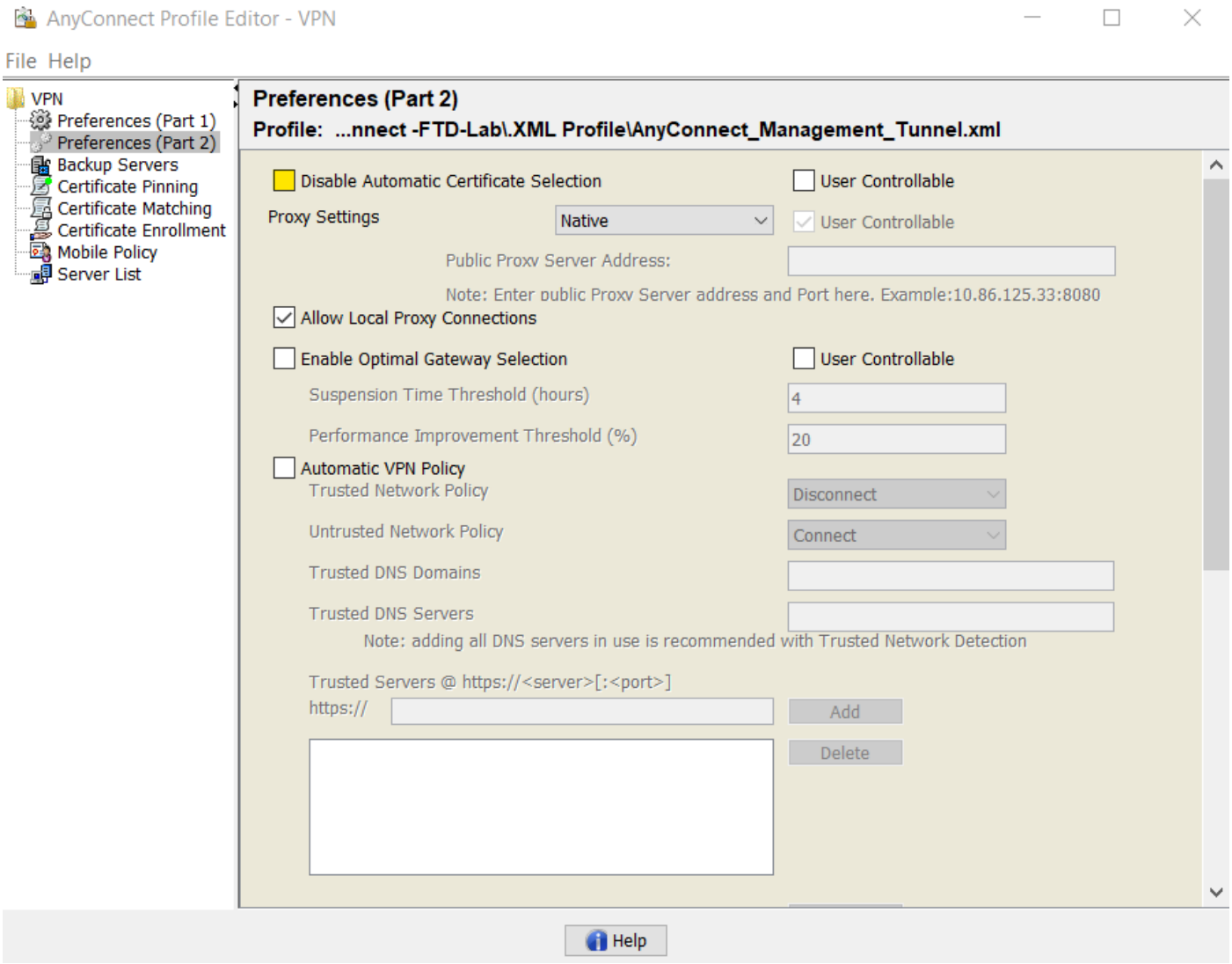
Además de la lista de servidores, el perfil de VPN de administración debe contener algunas preferencias obligatorias:

- **AutomaticCertSelection** debe establecerse en **true**.
- **AutoReconnect** debe configurarse en **true**.
- **AutoReconnectBehavior** se debe configurar para **ReconnectAfterResume**.
- **AutoUpdate** se debe establecer en **false**.
- **BlockUnTrustedServers** se debe establecer en **true**.
- **CertificateStore** debe configurarse para **MachineStore**.
- **CertificateStoreOverride** debe establecerse en **true**.
- **EnableAutomaticServerSelection** debe establecerse en **false**.
- **EnableScripting** se debe establecer en **false**.
- **RetainVPNOnLogoff** debe configurarse en **true**.

En el Editor de perfiles de AnyConnect, vaya a **Preferencias (Parte 1)** y ajuste la configuración de la siguiente manera:



A continuación, navegue hasta **Preferencias (Parte 2)** y desmarque la **opción Desactivar selección automática de certificados**.



Paso 2. Crear perfil VPN de AnyConnect

Además del perfil de VPN de administración, se debe configurar el perfil VPN normal de AnyConnect. El perfil VPN de AnyConnect se utiliza en el primer intento de conexión; durante esta sesión, el perfil VPN de administración se descarga desde FTD.

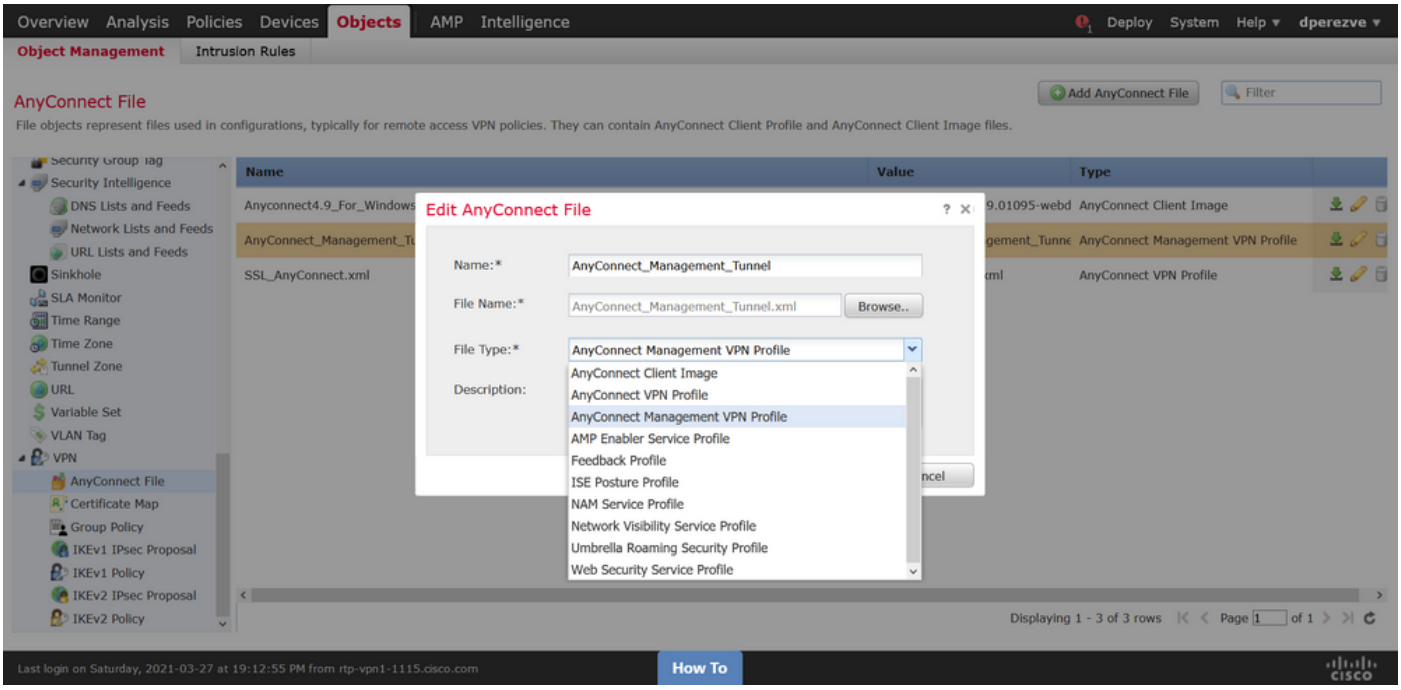
Utilice el Editor de perfiles de AnyConnect para crear el perfil VPN de AnyConnect. En este caso, ambos archivos contienen la misma configuración, por lo que se puede seguir el mismo procedimiento.

Paso 3. Cargue el perfil VPN de administración de AnyConnect y el perfil VPN de AnyConnect en FMC

Una vez creados los perfiles, el siguiente paso es cargarlos en el FMC como objetos de archivo AnyConnect.

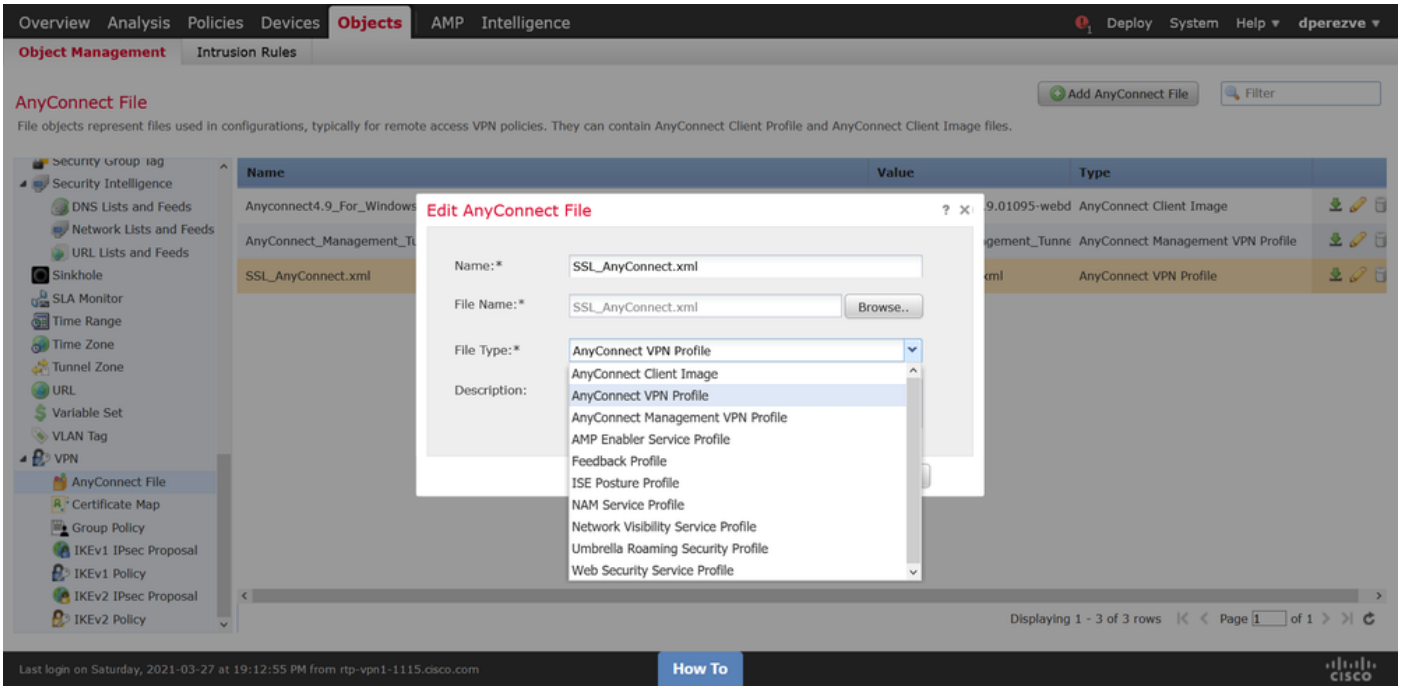
Para cargar el nuevo perfil VPN de administración de AnyConnect en FMC navegue a **Objetos > Administración de objetos** y elija la opción **VPN** de la tabla de contenido, luego seleccione el **botón Add AnyConnect File**.

Proporcione un nombre para el archivo, elija **AnyConnect Management VPN Profile** como tipo de archivo y guarde el objeto.

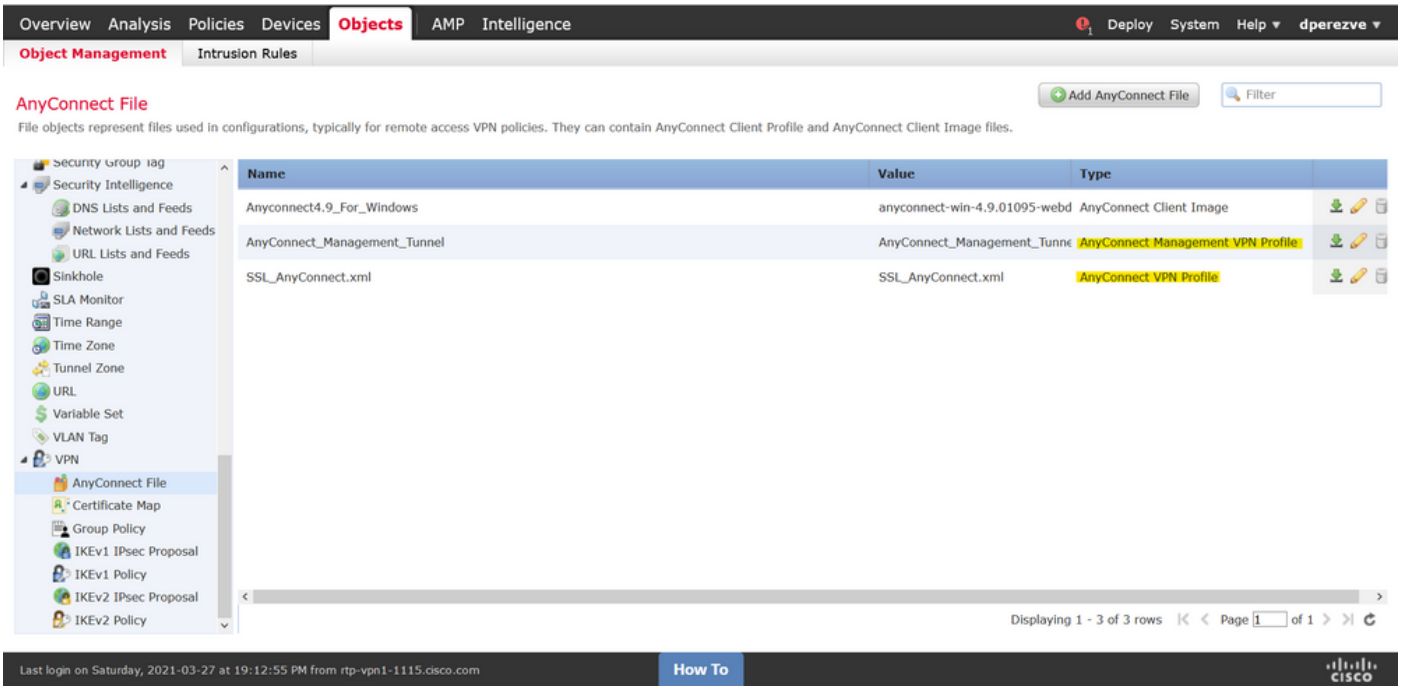


Ahora, para cargar el perfil de VPN de AnyConnect navegue de nuevo a **Objetos > Administración de objetos** y elija la opción **VPN** de la tabla de contenido, luego seleccione el botón **Agregar archivo de AnyConnect**.

Proporcione un nombre para el archivo, pero esta vez elija **AnyConnect VPN Profile** como tipo de archivo y guarde el nuevo objeto.



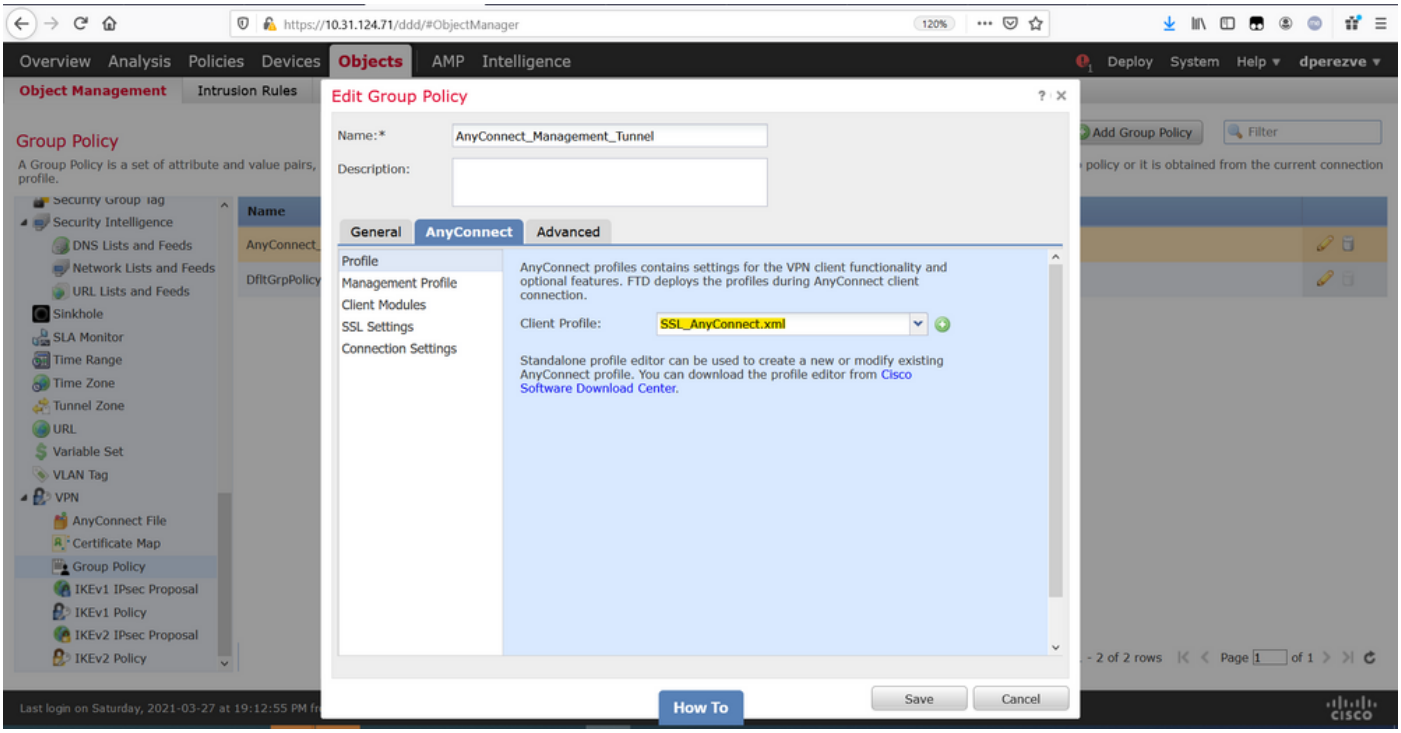
Los perfiles se deben agregar a la lista de objetos y marcar como **AnyConnect Management VPN Profile** y **AnyConnect VPN Profile** respectivamente.



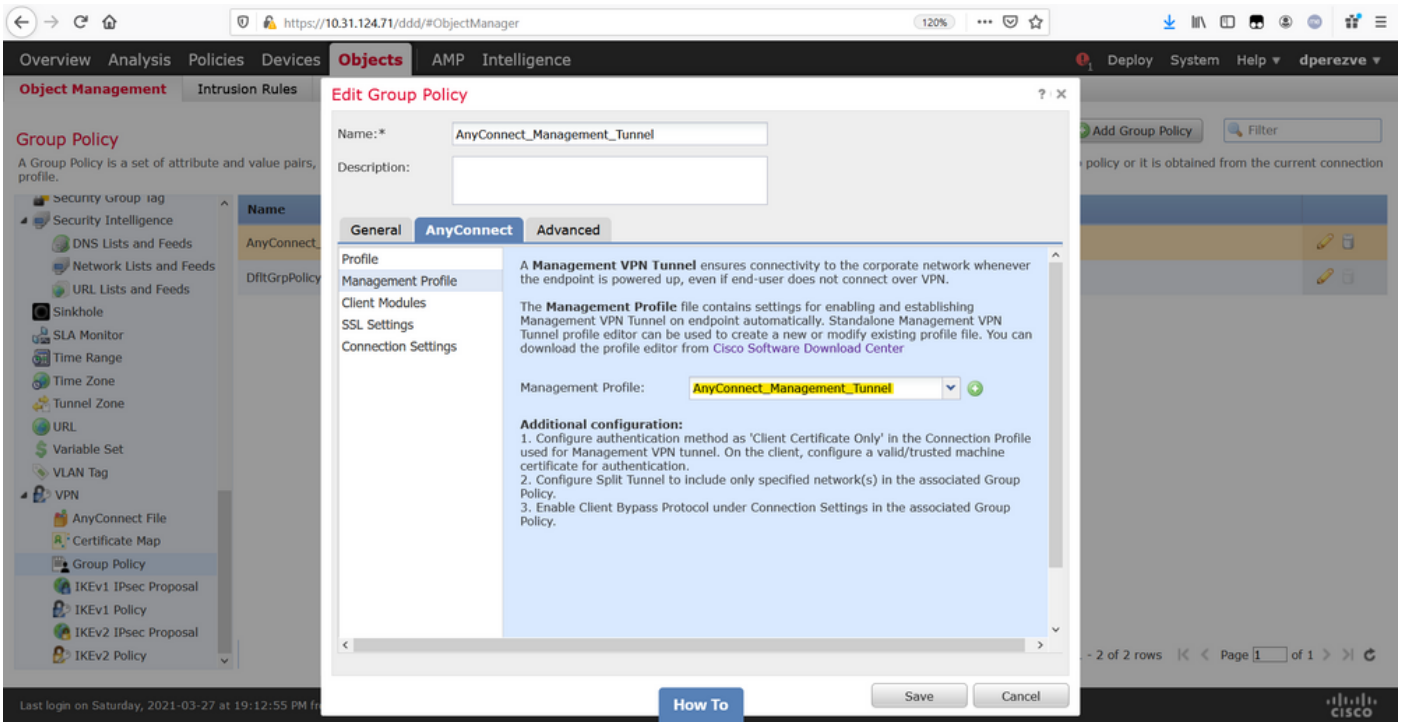
Paso 4. Crear política de grupo

Para crear una nueva política de grupo, navegue hasta **Objetos > Administración de objetos** y elija la opción **VPN** de la tabla de contenido, luego seleccione **Política de grupo** y haga clic en el **botón Agregar política de grupo** .

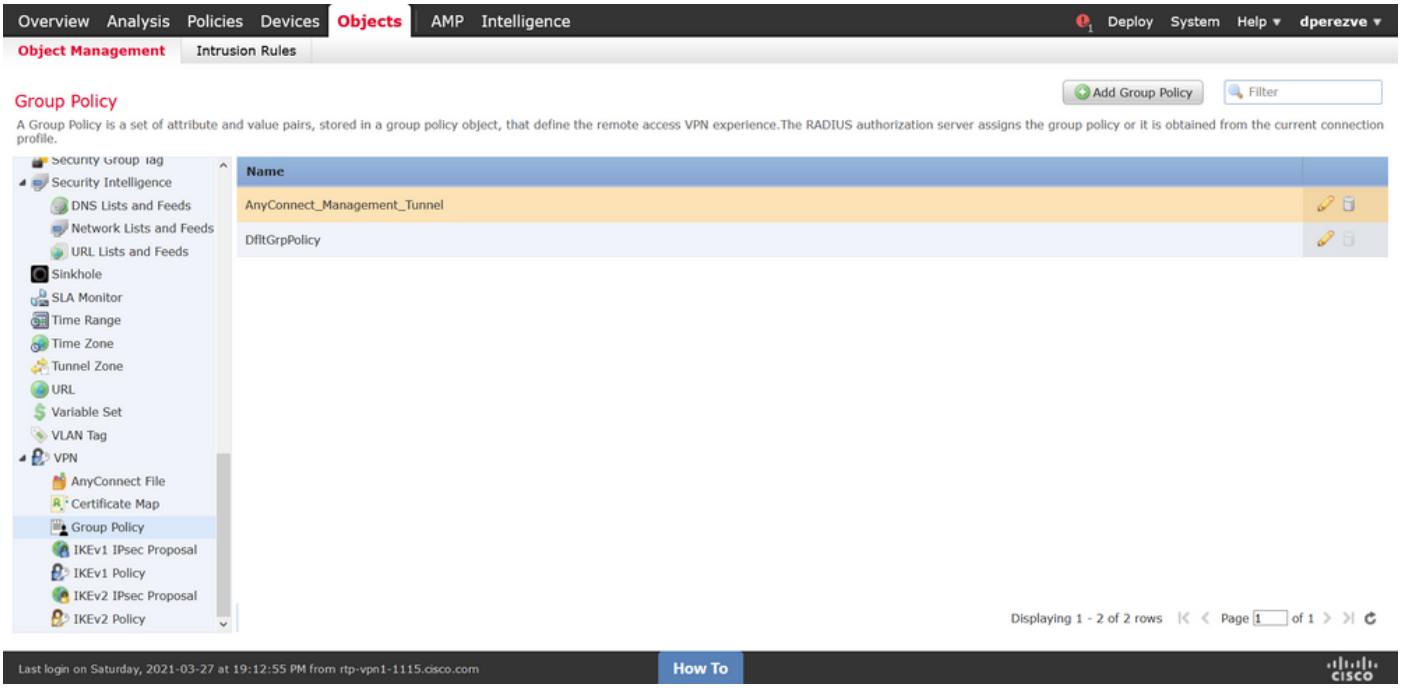
Una vez que se abra la ventana **Agregar política de grupo**, asigne un nombre, defina un grupo de AnyConnect y abra la pestaña **AnyConnect**. Navegue hasta **Profile** y seleccione el objeto que representa el perfil VPN normal de AnyConnect en el menú desplegable **Client Profile**.



A continuación, navegue hasta la ficha **Perfil de administración** y seleccione el objeto que contiene el perfil de VPN de administración en el menú desplegable **Perfil de administración**.



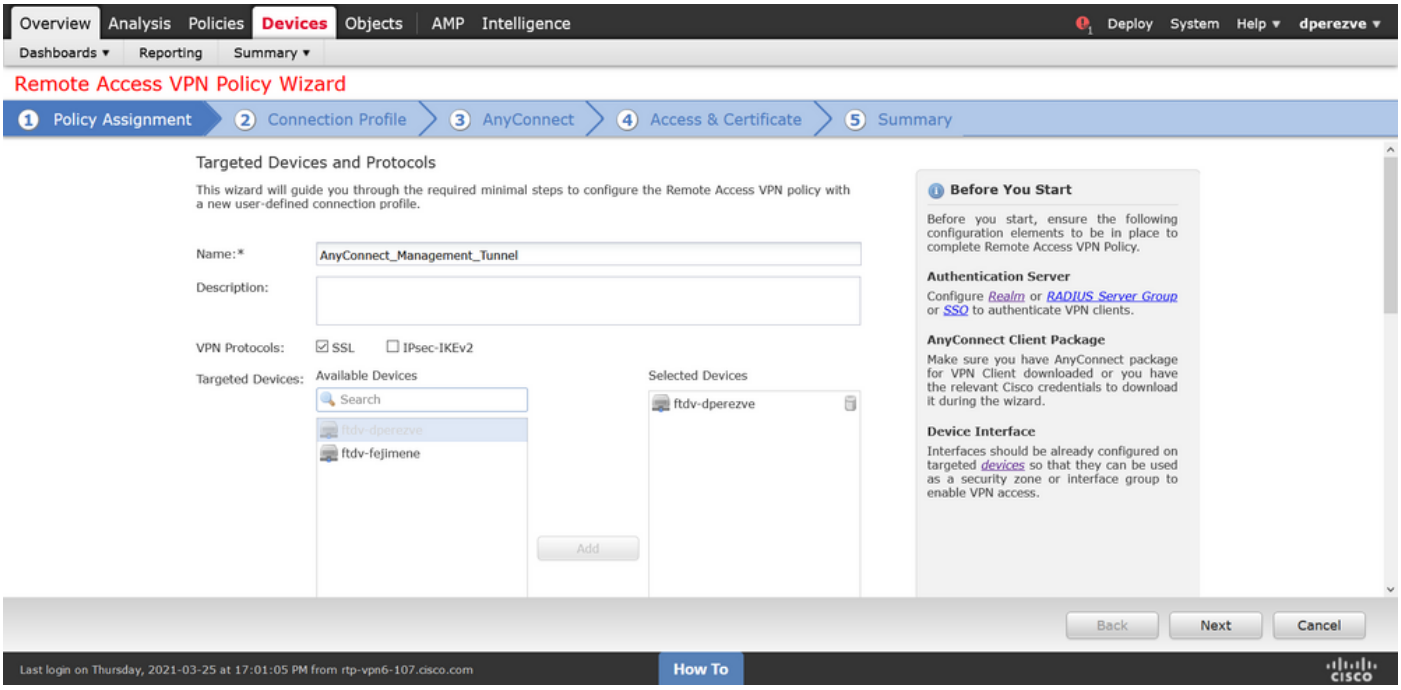
Guarde los cambios para agregar el nuevo objeto a las directivas de grupo existentes.



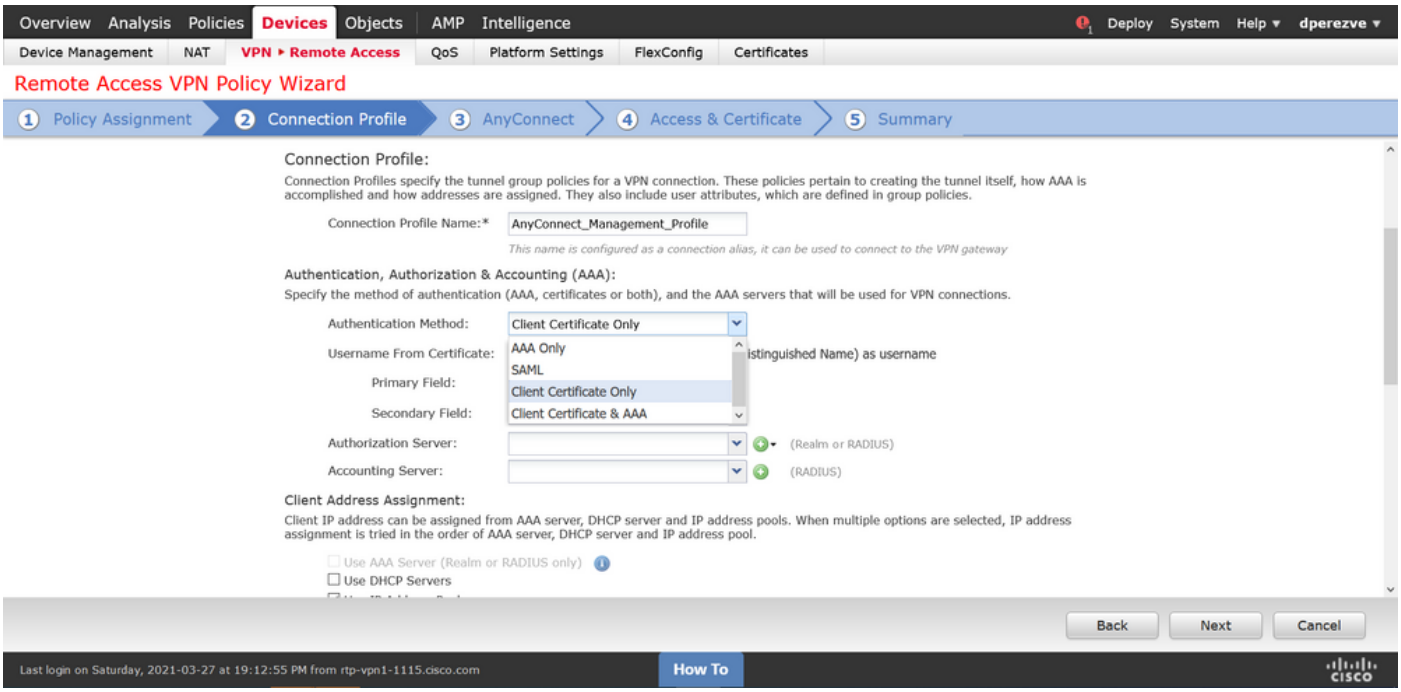
Paso 5. Crear nueva configuración de AnyConnect

La configuración de SSL AnyConnect en FMC consta de 4 pasos diferentes. Para configurar AnyConnect, navegue hasta **Devices > VPN > Remote Access** y seleccione el **botón Add** . Esto debe abrir el **Asistente de Políticas de VPN de Acceso Remoto**.

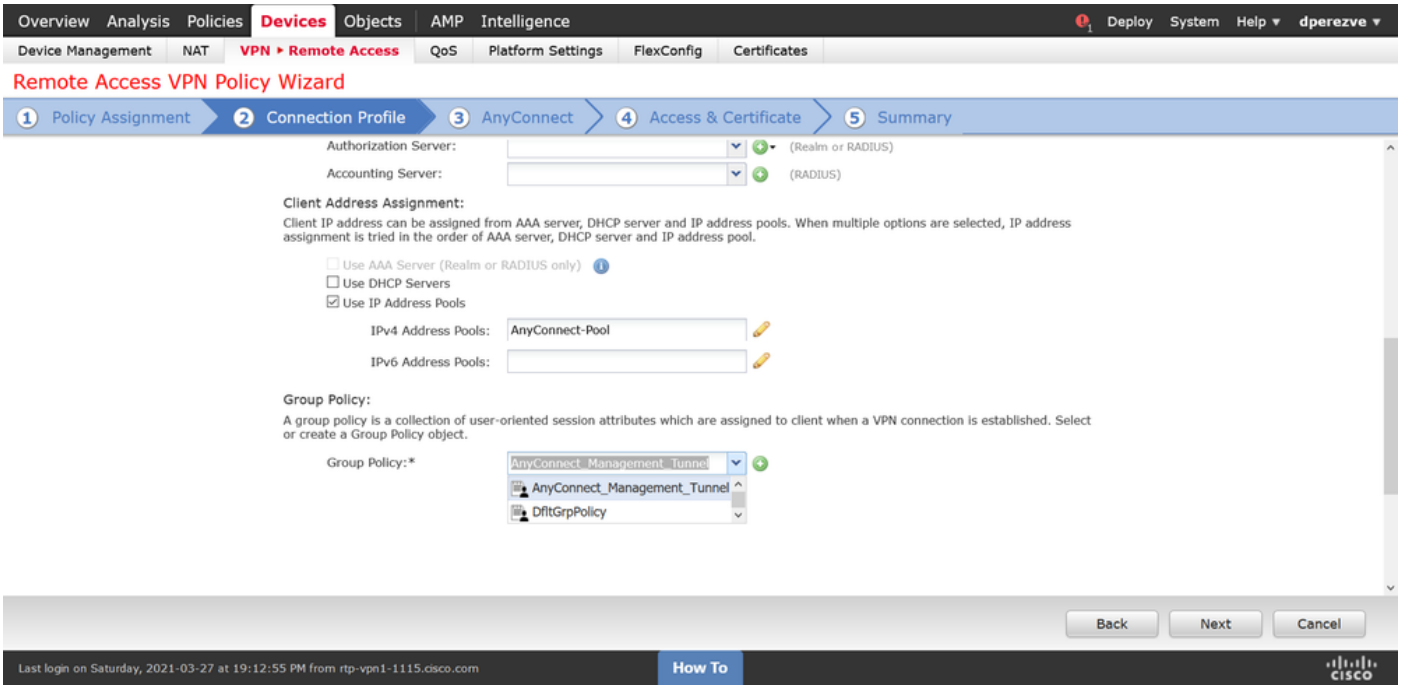
En la pestaña **Asignación de políticas** seleccione el dispositivo FTD que se encuentra en la mano, defina un nombre para el perfil de conexión y marque la casilla de verificación SSL.



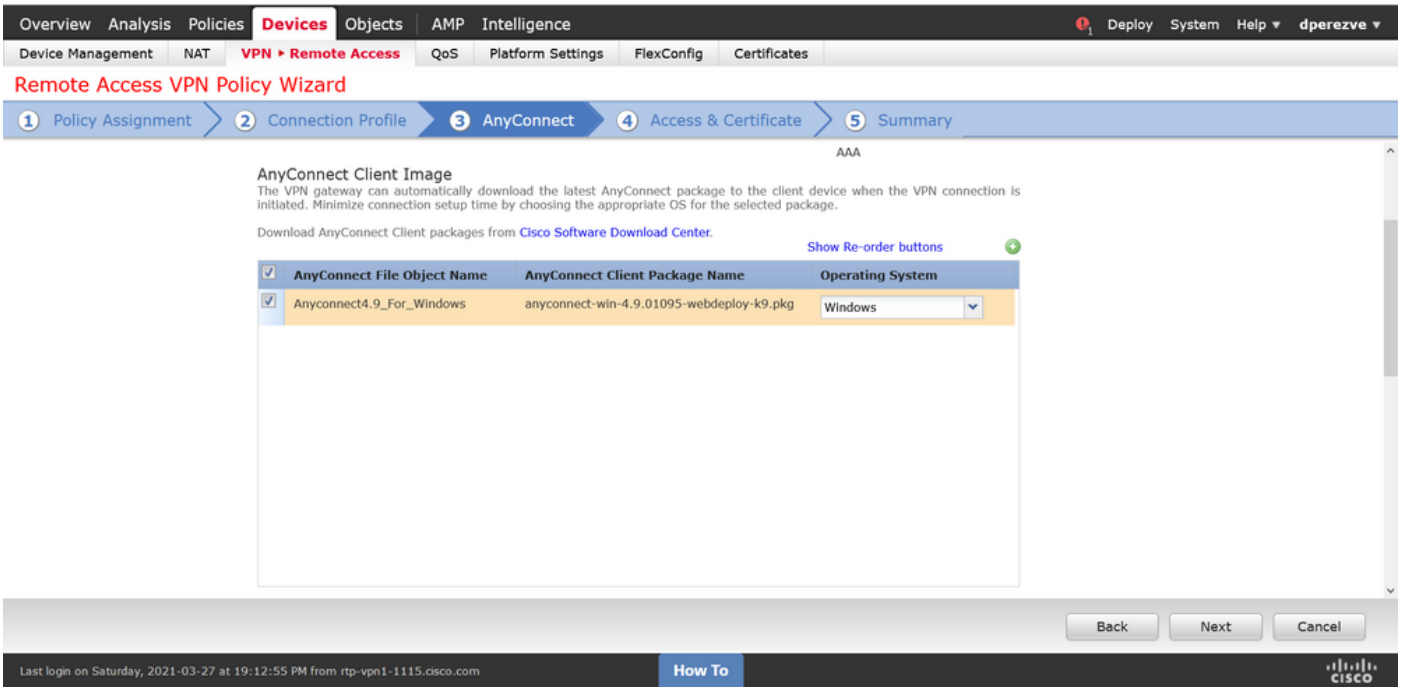
En **Perfil de conexión** seleccione **Certificado de cliente solamente** como método de autenticación. Esta es la única autenticación admitida para la función.



A continuación, seleccione el objeto Group Policy creado en el paso 3 en el menú desplegable **Group Policy**.



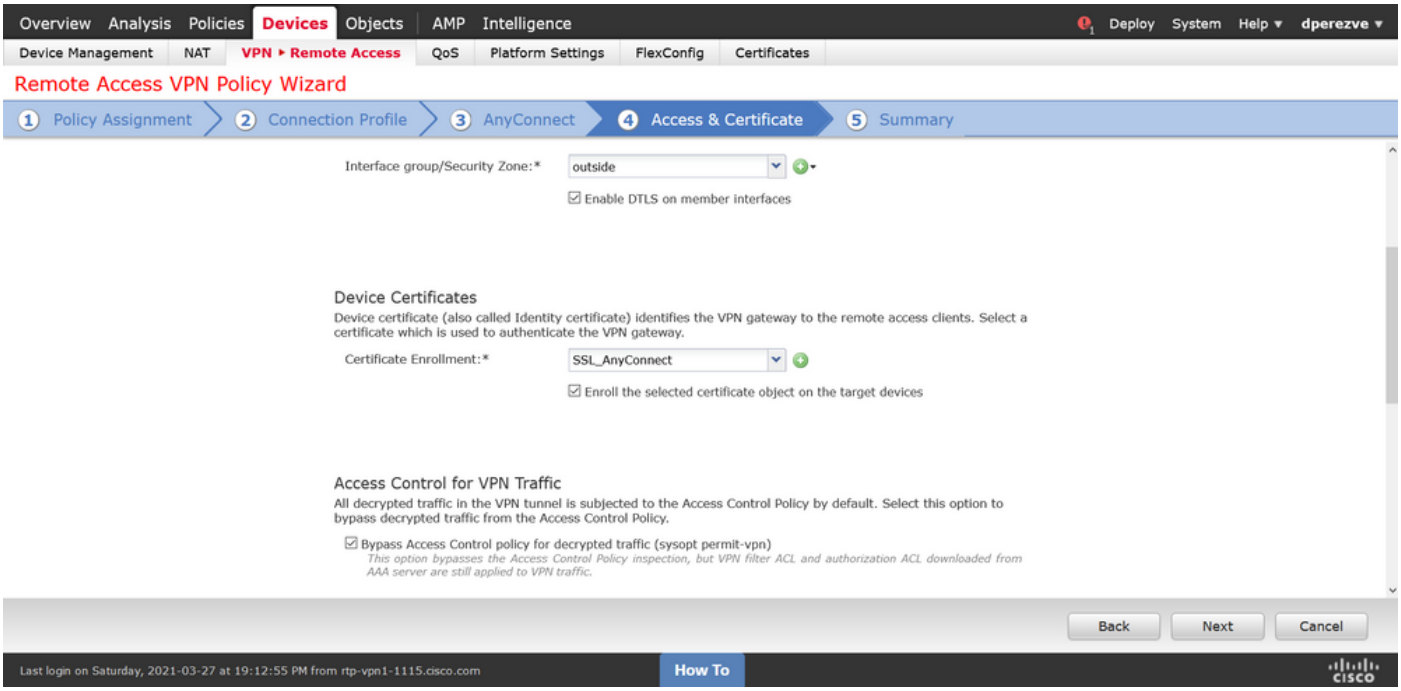
En la ficha **AnyConnect**, seleccione el **objeto de archivo AnyConnect** según el sistema operativo (SO) del terminal.



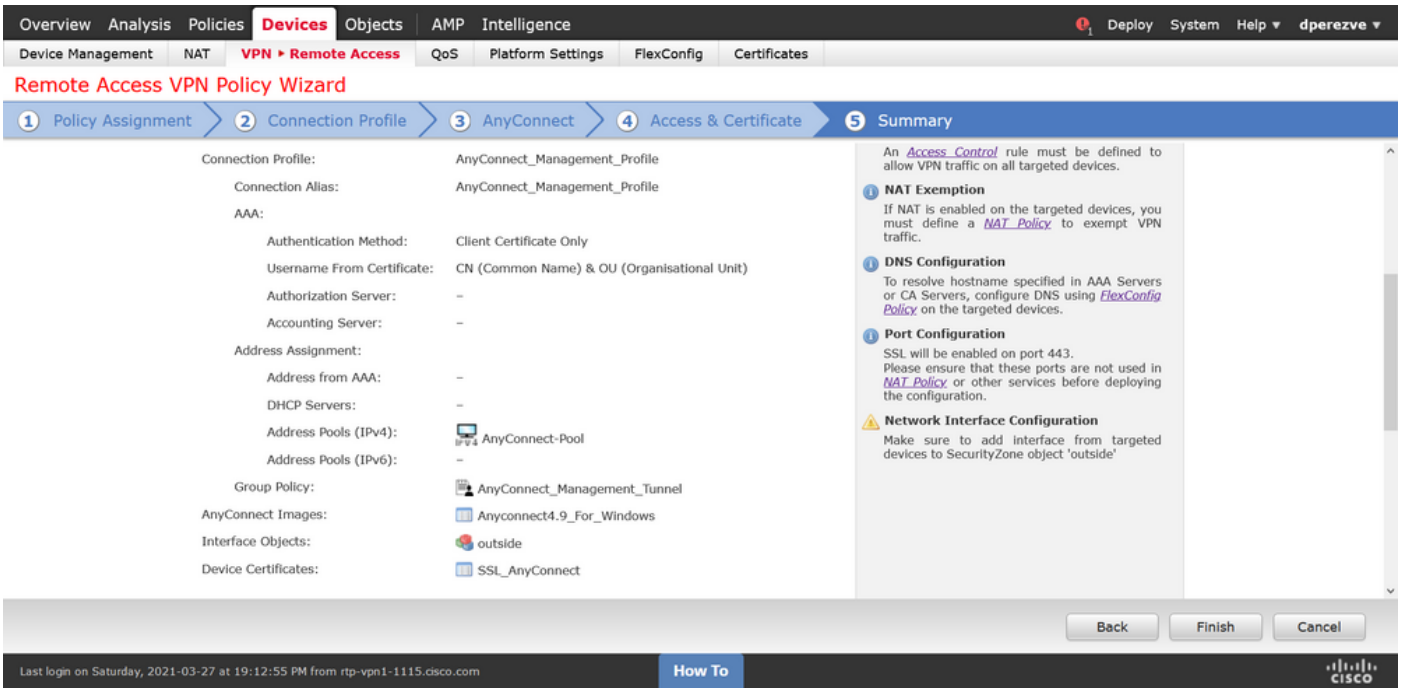
En **Access & Certificate** especifique el certificado que debe utilizar FTD para sondear su identidad al cliente de Windows.

> **Nota:** Dado que los usuarios no deben interactuar con la aplicación AnyConnect cuando utilizan la función Management VPN, el certificado debe ser de plena confianza y no debe imprimir ningún mensaje de advertencia.

> **Nota:** Para evitar errores de validación de certificados, el campo Nombre común (CN) incluido en el Nombre de asunto del certificado debe coincidir con el FQDN definido en la lista de servidores de perfiles XML (Paso 1 y Paso 2).



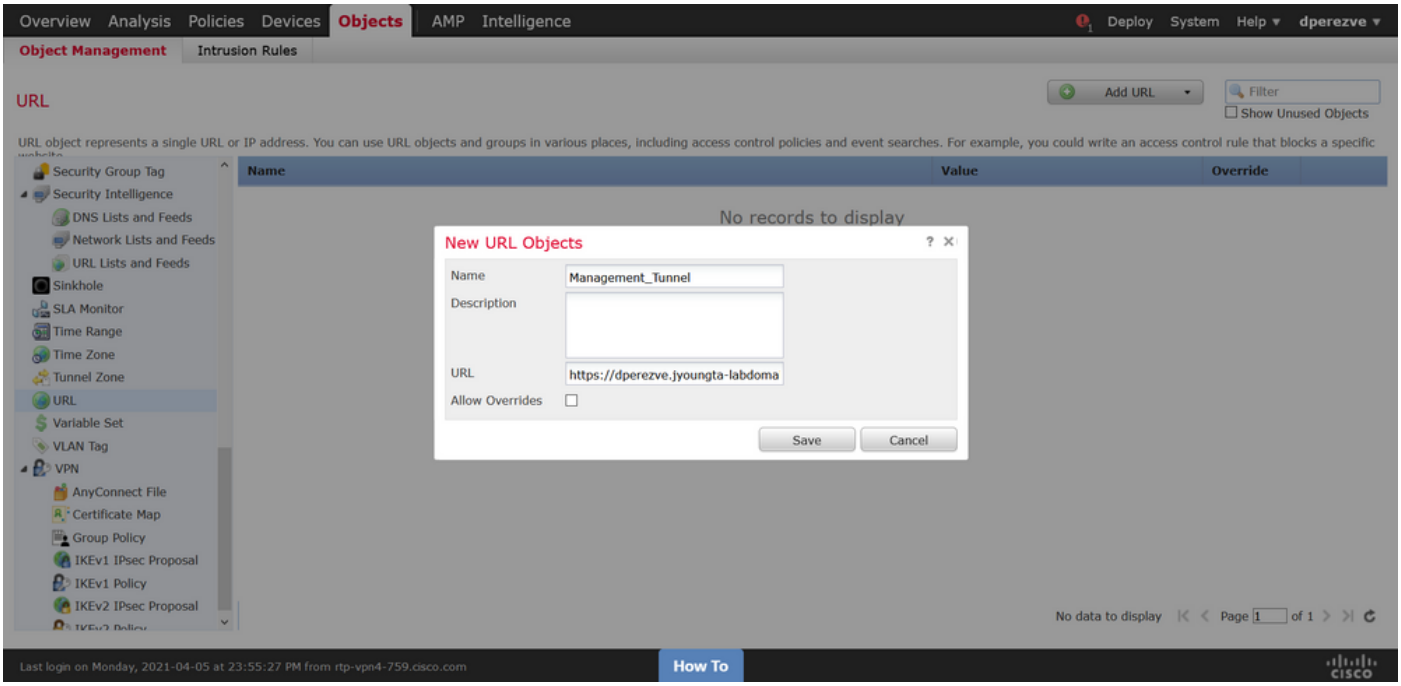
Por último, seleccione el botón **Finalizar** en la pestaña **Resumen** para agregar la nueva configuración de AnyConnect.



Paso 6. Crear objeto URL

Navegue hasta **Objetos > Administración de objetos** y seleccione **URL** en la tabla de contenido. A continuación, seleccione **Agregar objeto** en el menú desplegable **Agregar URL**.

Proporcione un nombre para el objeto y defina la dirección URL utilizando el mismo FQDN/grupo de usuarios especificado en la lista de servidores de perfiles de VPN de administración (paso 2). En este ejemplo, la URL debe ser dperezve.jyoungta-labdomain.cisco.com/AnyConnect_Management_Tunnel.



Guarde los cambios para agregar el objeto a la lista de objetos.

Paso 7. Definir alias de URL

Para habilitar el Alias de URL en la configuración de AnyConnect, navegue hasta **Devices > VPN > Remote Access** y haga clic en el icono del lápiz para editarlo.

A continuación, en la ficha Perfil de conexión, seleccione la configuración que desee, navegue hasta **Alias**, haga clic en el **botón Agregar** y seleccione el **objeto URL** en el menú desplegable Alias URL. Asegúrese de que la casilla de verificación **Enabled** esté activada.

Guarde los cambios e implemente configuraciones en FTD.

Verificación

Una vez finalizada la implementación, se necesita una primera conexión AnyConnect manual con el perfil VPN de AnyConnect. Durante esta conexión, el perfil de VPN de administración se descarga de FTD y se almacena en **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**. A partir de este punto, las conexiones subsiguientes se deben iniciar a través del perfil VPN de administración sin ninguna interacción del usuario.

Troubleshoot

Para errores de validación de certificados:

- Asegúrese de que el certificado raíz para la Autoridad de Certificación (CA) esté instalado en el FTD.
- Asegúrese de que un certificado de identidad firmado por la misma CA esté instalado en Windows Machine Store.
- Asegúrese de que el campo CN se incluye en el certificado y es el mismo que el FQDN definido en la lista de servidores del perfil VPN de administración y el FQDN definidos en el alias URL.

Para túnel de administración no iniciado:

- Asegúrese de que el perfil de VPN de administración se haya descargado y almacenado en **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\MgmtTun**.
- Asegúrese de que el nombre del perfil de VPN de administración sea **VpnMgmtTunProfile.xml**.

Para los problemas de conectividad, recopile el paquete DART y póngase en contacto con el TAC de Cisco para obtener más información.